GUIA DO USUÁRIO
SEGURANÇA DA INFORMAÇÃO

A segurança da nossa empresa é você quem faz

APRESENTAÇÃO

A informação é um ativo cada dia mais valorizado, pois representa um diferencial competitivo de grande importância estratégica para as organizações. Em uma sociedade na qual as Tecnologias da Informação são rapidamente difundidas, as organizações precisam se estruturar para lidar com questões como integridade, disponibilidade, confidencialidade e valor deste importante ativo.

À medida que as tecnologias da informação se fazem cada vez mais necessárias, a criação e manutenção de uma política que mantenha a informação íntegra, disponível e acessível a quem de direito torna-se imprescindível. A política de Segurança da Informação visa preservar o valor do ativo e diminuir os riscos inerentes ao seu uso.

Nas páginas a seguir serão apresentados diversos itens das *Normas de Segurança da Informação*, que são os elementos de execução da Política de Segurança da Informação implantada na Instituição.

CONTAS E SENHAS

- *A senha é sua assinatura eletrônica.*
- *Mantenha sigilo absoluto, não revele e não anote sua senha, memorize-a.*
- *Não utilize números que possuem ligação com você como: telefone, RG, CPF/CNPJ, data de nascimento (para cartões de débito e crédito, fone fácil, etc.).*
- *Não utilize composições com números repetidos, ou seqüências como: 1112233, 157157, 1234321.*

Uma senha *password* na Internet, ou em qualquer sistema computacional, serve para autenticar o usuário, ou seja, é utilizada no processo de verificação da identidade do usuário, assegurando que este é realmente quem diz ser.

1. Todos os usuários de recursos de informação devem conhecer a Política de Segurança da Informação da Instituição no momento de sua contratação (empregados, estagiários e prestadores de serviços).
2. As contas de acesso dos prestadores de serviços possuirão prazo de validade de acordo com a vigência do contrato de estágio e trabalho com a Instituição.
3. A inclusão/exclusão de contas de usuário da rede e dos sistemas deve ser solicitadas à Assessoria de Informática, através do coordenador da área (superior imediato do usuário) informando se houve contratação, contratação temporária, suspensão de contrato, afastamento provisório, à disposição, etc. Cada coordenador também é responsável por monitorar e informar à Assessoria de Informática os casos de contratações e desligamentos, para que sejam liberados/bloqueados os acessos aos sistemas.
4. É proibida a conexão de equipamentos não autorizados à rede local da Instituição. Quando necessária, a conexão deve ser autorizada pela Assessoria de Informática. Deverá também, possuir especificações de hardware homologadas e ferramentas que garantam a integridade das informações da Instituição.
5. Os acessos externos às Redes Corporativas somente serão permitidos a equipamentos homologados e cadastrados pela Assessoria de Informática.
6. Ao se afastar da estação de trabalho, o usuário deve encerrar ou bloquear a sessão com “logoff”, evitando que outras pessoas acessem os sistemas com a sua senha.
7. É proibido o cadastro de contas impessoais, tais como: guest, visitante, backup, operador, super, etc. As exceções a esta regra deverão ser avaliadas pelo Diretor ou Coordenador diretamente interessado pela exceção e a Assessoria de Informática.
8. Não devem ser adotados para senha: datas, nomes próprios, palavras constantes em dicionários e siglas.
9. As senhas devem ter no mínimo 08 (oito) caracteres e sempre que possível deve-se misturar letras, números e caracteres especiais (!, ?, #, etc.). Não devem ser utilizadas como senhas palavras que façam parte

de dicionários (inglês, português, espanhol, francês e etc.), uma vez que são de fácil dedução pelos programas de quebra de senha.

Como elaborar uma boa senha?
Quanto mais "bagunçada" for a senha melhor, pois mais difícil será descobri-la. Assim, tente misturar letras maiúsculas e minúsculas, números e sinais de pontuação. Uma regra realmente prática e que gera boas senhas difíceis de serem descobertas é utilizar uma frase qualquer e pegar a primeira, segunda ou a última letra de cada palavra.

10. A reutilização de senhas obedecerá ao ciclo mínimo de 05 (cinco) trocas, ou seja, as últimas 05 (cinco) senhas não poderão ser reutilizadas.
11. O usuário terá direito a 04 (quatro) tentativas de autenticação de senha, sendo todas mal sucedidas, será bloqueado o acesso ao sistema.
12. Em caso de impossibilidade de acesso, a Assessoria de Informática deve liberá-lo após autorização formal do coordenador do usuário.
13. A senha possui validade de 90 dias, e sua troca será solicitada automaticamente quando da expiração da mesma.
14. É expressamente proibida a divulgação de senha. Em caso de suspeita da perda de sigilo, ela seve ser trocada imediatamente.

Quantas senhas diferentes devo usar?
Este número deve ser equivalente à quantidade de contas distintas a serem mantidas por você. Imagine que você é responsável por realizar movimentações financeiras em um conjunto de contas bancárias e todas estas contas possuam a mesma senha. Antes de divulgar sua senha para alguém faça as seguintes perguntas:

- *Quais seriam as conseqüências se alguém utilizasse esta senha indevidamente?*
- *Como apurar um fato, se várias pessoas conhecem a minha senha?*
- *E se elas fossem diferentes, uma para cada conta? Caso alguém descobrisse uma das senhas, o prejuízo teria a mesma proporção?*

15. Haverá bloqueio automático da senha nos sistemas após 90 dias sem a utilização da mesma.

ACESSO, MANUSEIO E TRANSPORTE DA INFORMAÇÃO

- *Sigilo e privacidade são duas palavras-chave quando se trata de divulgação de informações.*
- *Uma das conseqüências da divulgação não autorizada de informação é a perda de oportunidades estratégicas.*
- *O vazamento de algumas informações podem comprometer a imagem da empresa.*

Uso das Informações

1. Somente pessoal autorizado deve utilizar os recursos de informática, ou seja, o seu uso deve ser limitado aos interesses da organização.
2. Todo acesso aos recursos de informações da Instituição serão controlados e registrados em arquivo de log, assim como o acesso à rede. Em se tratando de informações críticas, o registro do log, se torna obrigatório.
3. O usuário deve manter sigilo sobre as informações estratégicas e confidencias, de acordo com a norma de classificação das informações.
4. O usuário é responsável pelas informações armazenadas nos equipamentos de uso exclusivo. Nos casos de equipamentos de utilização coletiva, a responsabilidade é do coordenador da unidade, ou pessoa por ele designada.
5. As informações classificadas como críticas, que serão disponibilizadas para realização de trabalho fora das dependências da Instituição, sejam elas via e-mail, disquetes ou outro meio eletrônico, deverão conter senhas, e/ou utilizar criptografia para que seja garantida a integridade, a disponibilidade e a confidencialidade. Em caso de dúvida solicitar maiores informações à Assessoria de Informática.
6. O usuário deve informar ao seu coordenador quando informações ou aplicações críticas forem encontradas sem tratamento de segurança correto. O coordenador deve informar a ocorrência à Assessoria de Informática.
7. Caso o usuário se ausente da sua estação de trabalho por um período superior a 05 (cinco) minutos, deve ser ativada a proteção de tela com senha. Para configurar esta opção, o usuário deverá acionar a Assessoria de Informática. O usuário deve encerrar a sua sessão na estação de trabalho ao final do expediente.

Fique por dentro...
Vulnerabilidade *é definida como uma falha no projeto ou implementação de um software ou sistema operacional, que quando explorada por um atacante resulta na violação da segurança de um computador.*

Existem casos onde um software ou sistema operacional instalado em um computador pode ter uma vulnerabilidade que permite sua exploração remota, ou seja, através da rede. Portanto, um atacante conectado à Internet, ao explorar tal vulnerabilidade, pode obter acesso não autorizado ao computador vulnerável.

8. A Assessoria de Informática é o responsável pela criação de condições eficientes, seguras e controladas para execução de aplicativos e armazenamento de informações confidenciais ou críticas que estejam sob sua administração.
9. É expressamente proibida a utilização de recursos de informação não autorizados ou não homologados pela Assessoria de Informática.
10. As informações críticas e estratégicas devem ser armazenadas nos servidores da Rede Corporativa. As restritas e confidenciais não devem ser armazenadas em diretórios públicos da rede (discos L ou T) ou estações de trabalho do usuário. Deverão ser gravadas no disco privado das redes (discos G ou I).

- Compete ao coordenador

1. Informar à Assessoria de Informática ou empresa gestora dos sistemas e banco de dados, o nível de privilégio de acesso e uso que os empregados, estagiários e prestadores de serviços de sua área necessitam, assim como sua exclusão de acesso.
2. Zelar pelo uso correto das informações sob a guarda dos empregados, estagiários e prestadores de serviços de sua área.

- Uso de software/hardware

1. A utilização de programas, aplicativos e softwares em geral devem ser restritos apenas aos autorizados, homologados e de acordo com a lei. É terminantemente proibido o uso de quaisquer outros programas não homologados ou autorizados pela Assessoria de Informática.
2. O usuário é o responsável pelo uso de software não autorizados ou não homologados.
3. O usuário deve sempre acompanhar a realização de manutenção preventiva ou corretiva de um recurso sob sua responsabilidade, quando esta for realizada no ambiente da Instituição.
4. As redes deverão possuir ferramentas com recursos de seguranças incorporados, definidos pela Assessoria de Informática.
5. A CPU, a memória, o espaço em disco, a placa de rede de servidores e a taxa de link remoto deverão ser constantemente monitorados pela Assessoria de Informática, visando manter a disponibilidade das informações.

- Controle de acesso e identificação

1. Os acessos do usuário aos recursos de informação são realizados através de sua identificação no ambiente informatizado, por isso é fundamental guardar as senhas em sigilo.
2. O compartilhamento dos recursos de informação, como unidades de CD-RW, diretórios (pastas) de trabalho das estações e outros dispositivos, deve ser evitado e, quando utilizados, o usuário deverá configurar para grupos restritos.

3. A Assessoria de Informática e a Diretoria Executiva são, respectivamente, os responsáveis por analisar e homologar os treinamentos relacionados a aspectos de Segurança da Informação.

- É expressamente proibida

1. A utilização de recursos de informação que contenham material obsceno, apologia ao fanatismo, qualquer forma de discriminação ou material que, explícita ou implicitamente, refira-se uma conduta imoral.
2. A posse, o acesso e a divulgação de informação que ameace a integridade física ou moral de outras pessoas ou organizações.
3. A posse e a utilização indevida de qualquer informação obtida através da rede corporativa.
4. A cópia não autorizada de software e sistemas adquiridos ou desenvolvidos pela Instituição, sem autorização da Diretoria Executiva.
5. A utilização, para interesses particulares, de hardware e software adquiridos ou desenvolvidos pela Instituição, bem como qualquer informação sob guarda das mesmas.
6. A instalação e o uso de softwares não licenciados ou não homologados pela Assessoria de Informática.

- Descarte de Informações

1. Devem ser removidos da rede os arquivos que não sejam mais necessários ou que não se refiram a assuntos de trabalho. Os arquivos serão mantidos no servidor por um período, de acordo com procedimentos específicos.
2. O processo de descarte das informações deve ocorrer de forma irrecuperável.

- Auditoria

1. Devem ser registradas, para efeito de controle e auditoria, as tentativas de conexões remotas, assim como, o início e o término de acessos à banco de dados, Internet e aplicativos.
2. Será dado o direito à Assessoria de Informática de realizar auditoria em todos os recursos de informação.
3. As auditorias poderão também ser realizadas a partir de solicitações do coordenador , através da análise conjunta com a Assessoria de Informática.
4. Os relatórios de auditoria serão encaminhados para os Coordenadores/Diretoria das respectivas áreas auditadas.

CORREIO ELETRÔNICO

As mensagens trafegam de uma máquina a outra aberta e disponíveis, como as mensagens escritas no dorso dos cartões postais: qualquer indivíduo localizado em uma máquina intermediária pode ler as mensagens, do mesmo modo que um carteiro pode ler o verso dos cartões postais manuseados.
A única segurança que o usuário do correio eletrônico tem baseia-se na honestidade, ignorância e indiferença daqueles situados nos pontos intermediários. Tais pontos podem ser desde universidades até empresas rivais ou governos estrangeiros. Um espião ou hacker poderá imprimir o e-mail, mostrá-lo a um amigo, despachá-lo pela rede ou mandar uma cópia à imprensa ou alterar a mensagem em trânsito.

O desejo de se comunicar é, sem dúvida, a essência das redes. As pessoas sempre procuraram se corresponder da maneira mais rápida e fácil possível. O correio eletrônico, ou e-mail, das redes de computadores é a aplicação que mais ilustra este anseio, pois reúne estes dois atributos. Além disso, não é necessário preocupar-se como a mensagem será entregue ao destinatário, da mesma forma que não precisamos conhecer como o sistema telefônico funciona internamente para utilizá-lo. Diante destes fatos, podemos concluir que o correio eletrônico é o principal, mais popular e mais usado serviço de rede. Porém, devemos estar atentos para a sua utilização. Vejamos a seguir algumas dicas e critérios:

1. A utilização do correio eletrônico deve ser restrita às atividades de interesse da empresa.
2. Considerando que o correio eletrônico é um meio de comunicação corporativo e reflete externamente a imagem da empresa, deve ser utilizada uma linguagem formal e deve ser evitado o uso de marcas, símbolos, logomarcas e slogans de campanhas internas, a não ser a logomarca oficial da empresa.
3. O uso do correio eletrônico através da Internet/intranet é dirigido para empregados, estagiários e prestadores de serviços que, no desempenho de suas atividades, necessitem comunicar-se internamente ou com outras empresas.
4. É de responsabilidade do coordenador designar as pessoas que devem ter acesso às contas de correio eletrônico, ligadas à Internet/intranet, enviando mensagens externas e internas para se comunicar com seus fornecedores, parceiros, clientes, etc., avaliando a real necessidade desse acesso.
5. Mensagens oriundas da Internet que não são de interesse da empresa não devem ser repassadas através do correio eletrônico corporativo. O mesmo vale para mensagens sobre vírus ou ameaças de segurança que aconselham o repasse das mensagens para outras pessoas. Nestes casos, o usuário deve eliminar a mensagem e jamais repassar internamente na empresa.

- Quem solicita uma conta de correio eletrônico?

6. Cabe ao coordenador solicitar a criação de uma nova conta de correio com a justificativa e os dados do empregado, estagiário ou prestador de serviço.

- Contas de correio e mensagens

7. As mensagens transmitidas pelo correio eletrônico não devem conter dados e informações confidenciais ou vitais da empresa, a não ser que adequadamente protegidas por senha ou criptografia. Em hipótese alguma o usuário pode emitir opinião, via correio eletrônico, como se fosse a da empresa, com exceção do órgão de comunicação interna ou corporativa, ou ainda o usuário que esteja formalmente autorizado pelo diretor da área.
8. É vedado ao usuário do correio eletrônico o envio de mensagens em nome de outra pessoa.
9. Cada usuário deve ter a sua própria conta de correio eletrônico, não devendo compartilhá-la com outra pessoa.
    a. O nome da conta de correio eletrônico deve obedecer a um padrão definido pela Assessoria de Informática, de maneira que seja identificado o nome e o sobrenome do usuário.
    b. Para as contas de correio eletrônico utilizadas por prestadores de serviço, deverá ser adotado procedimento que diferencie as mensagens enviadas por contratos temporários. O coordenador deverá orientar o prestador sob sua responsabilidade a utilizar na saudação das mensagens os seguintes itens: nome completo, nome da empresa a qual ele pertence e a expressão “a serviço da Celpos”.

E-mails são mensagens relativamente curtas entre duas pessoas. Não podem substituir uma reunião ou almoço de negócios.

10. O usuário não deve permitir que outra pessoa envie mensagens utilizando a sua caixa eletrônica. Caso o coordenador deseje que um subordinado administre seu correio, deve usar a delegação , onde consta que a mensagem foi passada por outra pessoa com a sua autorização.

- Conteúdo

11. O conteúdo de um correio eletrônico não pode conter mensagens abusivas, imagens obscenas, pornográficas, racistas, constrangedoras, difamatórias ou quaisquer comentários que possam desabonar a imagem da empresa ou de seus clientes.
    a. Não deve circular mensagem que, mesmo compactada, ultrapasse o tamanho de 3 (três) Mb. Para arquivos que exceda este tamanho, é recomendável enviar um e-mail aos usuários envolvidos informando o hiperlink do local específico da rede onde o arquivo pode ser consultado.

- Prestadores de serviços, Consultores e Estagiários

12. Os prestadores de serviços somente devem ter conta de correio eletrônico quando for estritamente necessário, notadamente para a execução de suas atividades, devendo a criação da conta ser autorizada pelo coordenador ao qual o serviço está vinculado.
13. O coordenador deve solicitar formalmente o acesso ao correio eletrônico para o prestador de serviço, consultor ou estagiário, indicando o término do contrato ou a exclusão do serviço para que seja programado o cancelamento no tempo devido, como também a saída antecipada desses empregados.

- Responsabilidades

14. Não é permitido disponibilizar o envio de correio eletrônico sem a identificação do emissor e não pode haver contas eletrônicas coletivas.
15. Toda mensagem criada e armazenada nos computadores ou redes é de propriedade da Instituição.
    a. Em caso de uso indevido do correio eletrônico, a Assessoria de Informática, mediante autorização expressa da Diretoria Executiva, reserva-se o direito de acessar o conteúdo dos correios eletrônicos dos empregados envolvidos.

Facilidade de identificação: o destinatário deve identificar rapidamente quem é o autor da mensagem e sobre o que ela trata.

16. É de responsabilidade do usuário informar à Assessoria de Informática mudanças cadastrais em caso de transferência de órgão e realizar as alterações no seu livro de endereço.
17. É obrigatória a troca de senha no primeiro acesso do usuário.
18. Não é permitido o compartilhamento de senhas. Em caso de perda de sigilo, a troca da mesma deve ser de responsabilidade do usuário.
19. O usuário deve administrar o seu espaço em disco, criando o hábito de realizar arquivamento na estação e eliminar da caixa de entrada/saída as mensagens antigas, a fim de proporcionar um bom desempenho dos servidores.
    a. No caso do Outlook/Netscape, as contas de correio devem ser configuradas para armazenamento nas estações, nunca no servidor.
20. É vedado ao usuário o direito de passar mensagens para toda empresa, evitando-se, assim, o congestionamento no tráfico de mensagens da rede, bem como a redução do número de mensagens nas caixas dos usuários. Mensagens com esta característica devem ser divulgadas pelo órgão de comunicação interna.

***Evite**:*

- *Enviar mensagens com grandes arquivos anexados;*
- *Repassar mensagens recebidas e correntes;*
- *Enviar e-mail para desconhecidos;*
- *Enviar mensagens com assuntos muito íntimos.*

21. O usuário deve certificar-se de que seu procedimento esteja sempre de acordo com os padrões éticos e profissionais quando da utilização do serviço de correio eletrônico, uma vez que os funcionários da Instituição são identificados através do endereço xxx@celpos.com.br, as mensagens são consideradas correspondências oficiais.
22. O usuário deve incluir uma retratação em todas as suas mensagens. As palavras recomendadas para este fim são: "*As informações existentes nessa mensagem e seus anexos são de uso restrito. Caso não seja destinatário desta mensagem, favor não copiar ou divulgar as informações, apagando-as e notificando ao remetente. O uso impróprio será tratado conforme a legislação em vigor*".
23. Todas as comunicações em fóruns profissionais devem estar de acordo com o copyright ou outras leis de propriedade intelectual.

- O que é proibido?

24. São expressamente proibidas as seguintes atividades:
    a. Transmissão de informações que impliquem em violação de quaisquer leis ou constituam incitamento de qualquer crime;
    b. Violação de direitos autorais, particularmente sobre software, dados e publicações;
    c. Posse e divulgação de informações que ameacem a integridade física ou moral de outras pessoas ou organizações;
    d. Posse e utilização indevida de qualquer informação obtida através da rede corporativa, seja por qualquer meio ou finalidade.

- Cuidado com o SPAM

SPAM é o termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas.

Quais são os problemas que o SPAM pode causar para um usuário da internet?

Os usuários do serviço de correio eletrônico podem ser afetados de diversas formas. Alguns exemplos são:

- Não recebimento de e-mails

Boa parte dos provedores de internet limita o tamanho da caixa postal do usuário no seu servidor. Caso o número de SPAMs recebidos seja muito grande, o usuário corre o risco de ter sua caixa postal lotada com mensagens não solicitadas. Se isto ocorrer, todas as mensagens enviadas, a partir deste momento, serão devolvidas ao remetente e o usuário não conseguirá mais receber e-mails até que possa liberar espaço em sua caixa postal.

- Gasto desnecessário de tempo

Para cada SPAM recebido, o usuário necessita gastar um determinado tempo para ler, identificar o e-mail como SPAM e removê-lo da caixa postal.

- Aumento de custos

Independentemente do tipo de acesso à internet utilizado, quem paga a conta pelo envio do SPAM é quem o recebe. Por exemplo, para um usuário que utiliza acesso discado à internet, cada SPAM representa alguns segundos a mais de ligação que ele estará pagando.

- Perda de produtividade

Para quem utiliza o correio eletrônico como uma ferramenta de trabalho, o recebimento de SPAMs aumenta o tempo dedicado à tarefa de leitura de e-mails, além de existir a possibilidade de mensagens importantes não serem lidas, serem lidas com atraso ou apagadas por engano.

- Conteúdo impróprio

Como a maior parte dos SPAMs são enviados para conjuntos aleatórios de endereços de e-mails, não há como prever se uma mensagem com conteúdo impróprio será recebida. Os casos mais comuns são de SPAMs com conteúdo pornográfico.

Mensagem personalizada

- *Uma prática comum e não muito recomendado é deixar visível a lista de pessoas para as quais você está remetendo o e-mail.*
- *No cabeçalho, evite as saudações barrocas como "ilustríssimo senhor" ou "excelentíssimos doutores".*
- *Mensagens muito longas correm o risco de não serem lidas, porque muitas vezes o destinatário abre, assusta-se com a quantidade de linhas e acaba "deixando para depois". Como a troca de mensagens é praticamente imediata, há casos em que pode ser melhor dividir o que você tem a dizer, estabelecendo prioridades. Espere a primeira resposta e depois continue o assunto em um novo e-mail.*
- *Não repasse simplesmente um e-mail que contenha alguma informação que você queira difundir, principalmente para um superior. Isso denota uma certa preguiça e impessoalidade. É delicado fazer uma introdução sua e mandar o corpo do texto em seguida.*
- *Se estiver mandando cópias, siga a hierarquia: a mensagem para o superior e as cópias para os demais.*
- *Não usar abreviaturas utilizadas em salas de bate-papo ou chats como: qq, vc, tb.*

INTERNET

- *Vacine todos os programas recebidos via download.*
- *Nunca envie informações pessoais e da empresa, em salas de bate-papos (chats).*
- *Nunca execute programas ou arquivos enviados por desconhecidos.*
- *Efetue backups de seus arquivos importantes.*
- *Ao efetuar qualquer tipo de compra, tenha certeza de que as informações repassadas à loja estejam criptografadas; deve aparecer um cadeado no site.*
- *Leia os documentos on-line sobre privacidade e segurança que os sites fornecem, antes de fazer qualquer transação.*

Hoje, vive-se um surto de tecnologias na era da internet. As empresas estão conectando-se a parceiros, clientes e mercados eletrônicos, o que aumenta os pontos de riscos e, consequentemente, as chances de incidentes e perdas de informações.

Então as minhas informações pessoais não estão seguras? ***Não****.*

Exemplo 1: algum desconhecido liga para a sua casa e diz ser do suporte técnico do seu provedor. Nesta ligação ele diz que sua conexão com a internet está apresentando algum problema e, então, pede sua senha para corrigi-lo. Caso você revele-a, este suporte técnico poderá realizar uma infinidade de atividades maliciosas, utilizando a sua conta de acesso à internet e, portanto, relacionando tais atividades ao seu nome.

Exemplo 2: você recebe uma mensagem de e-mail dizendo que seu computador está infectado por um vírus. A mensagem sugere que você instale um programa anexo, ou uma ferramenta disponível em um site de internet, para eliminar o vírus de seu computador. Na verdade, a real função desta ferramenta não é eliminar um vírus, mas sim permitir que alguém tenha acesso a seu computador e a todos os dados nele armazenados.

- Quais as normas para utilizar a internet na Instituição?

1. A internet e a intranet são consideradas aplicações críticas, devendo ser utilizadas de forma racional.
2. A utilização da internet e intranet deve ser liberada pela Assessoria de Informática, que deverá prover a utilização de meios que objetivem minimizar os riscos e vulnerabilidades inerentes à segurança.
3. A Instituição se reserva o direito de supervisionar uso de todos os seus serviços de computação, pois o acesso a WEB é oferecido pela Instituição para condução das atividades do negócio e auxílio no dia-a-dia das atividades profissionais, devendo ser utilizada de maneira eficaz e pró-ativa.
4. O acesso à internet só será permitido aos sites liberados e autorizados pela Instituição, de acordo com a norma, e será monitorado pela Assessoria de Informática.

5. A Instituição se reserva o direito de bloquear, sem aviso prévio, o acesso a sites cujo conteúdo não seja do seu interesse.
6. O usuário deve notificar à Assessoria de Informática caso encontre uma informação errada a respeito da Instituição ou de seus produtos na internet ou em qualquer outro fórum público.
7. Não é permitido utilizar os mesmos pares de login e senha da rede da Instituição para cadastrar-se em serviços providos na internet, ou seja, todos os identificadores e senhas para acesso aos sites da internet que requeiram registro de usuário (gratuitamente ou não) devem ser diferentes dos usados na Instituição.
8. O uso de internet deve ser apenas através da arquitetura segura definida pela Assessoria de Informática, utilizando-se de recursos firewall (software que serve como parede de proteção contra invasões externas à rede local).

- Qual o procedimento que deve ser adotado pelo empregado se receber mensagem interna com conteúdos pornográficos ou que atente contra a ética e a moral?

  Deverá comunicar ao seu coordenador imediato.

- E qual o procedimento da Instituição?

  Na falta do cumprimento da norma de internet, haverá uma comunicação direta ao usuário e ao superior imediato. A reincidência será comunicado ao diretor da área, para que sejam aplicadas as sanções administrativas previstas em normas internas e demais penalidades previstas na legislação em vigor.

- Como posso proteger minha senha?

  Como medida de segurança de sua senha, o usuário não deve:

  - Deixá-la exposta;
  - Fornecer a outras pessoas;
  - Facilitar para que sejam copiadas por outros;
  - Deixar de mudá-la regularmente.

- O que não é permitido?

- Fazer download de programas ou arquivos executáveis;
- Fazer cópias de materiais da internet, inclusive desenhos, artigos, gráficos, áudio, vídeo e fotografias sem autorização do proprietário ou citação da fonte;
- Acessar e divulgar informações que contenha material obsceno, apologia ao fanatismo, qualquer forma de discriminação ou material que, explícita ou implicitamente, refira-se a uma conduta imoral;
- Instalar e usar softwares não licenciados ou não homologados pela Assessoria de Informática.

SEGURANÇA FÍSICA DAS ESTAÇÕES

- *Apenas os técnicos credenciados podem realizar manutenções nos equipamentos.*
- *Nos microcomputadores residenciais, a placa de fax-modem permite a conexão com o provedor para acesso à internet. Já na empresa, a placa de fax-modem é um ponto de invasão utilizado pelos hackers, para ter acesso à rede corporativa.*
- *Jamais configure no seu computador a opção de compartilhamento "o mundo".*
- *Não permita que o seu equipamento seja utilizado para realizações de invasões.*

São máquinas para uso interno dos funcionários. Nestas máquinas, as principais medidas de segurança a serem tomadas são no intuito de evitar o acesso dos usuários não habilitados a áreas sensíveis do sistema.

1. Os equipamentos de informática terão identificação própria de inventário em local visível e não removível, onde, com base nesta identificação, será efetuado o controle de entrada e saída ou transferência do respectivo ativo.
2. A exclusão de informações consideradas críticas e confidenciais deve ser feita de modo a impossibilitar a recuperação das mesmas.

DICA: Esvazie sempre a lixeira de sua estação de trabalho.

3. A movimentação de recursos de informação de uma determinada área da Instituição deve ser autorizada pelo coordenador responsável, ou pelo gestor do contrato, quando se tratar de recursos de prestadores de serviços.

- Cuidado com o compartilhamento

A utilização de compartilhamento de diretórios (pastas) no Windows é bastante simples, porém a utilização desse tipo de recurso expõe o computador a uma grande quantidade de ataques pela rede. O principal ataque sobre compartilhamentos é feito pelos vírus de computador que se utilizam de falhas de segurança nos recursos de compartilhamento para se propagarem pela rede das empresas. Portanto, se você não quer ser infectado por vírus ou correr outros riscos de segurança, limite-se a compartilhar apenas impressoras, e para um grupo pequeno de pessoas; jamais usar a opção "ao mundo".

DICA: Quando tiver que compartilhar informações com o grupo de trabalho, utilize os discos corporativos da rede (I, T).

4. Caso seja necessária a remoção do equipamento para manutenção em ambiente externo, o responsável pelo seu uso deve certificar-se de que

este está sendo entregue isento de informações de natureza crítica, sigilosa ou reservada.

5. O uso de hardware deve ser restrito apenas aos autorizados e homologados.
6. A Assessoria de Informática deve avaliar a obsolescência dos equipamentos e planejar sua substituição.
7. A aquisição de hardware deve ser aprovada e gerenciada pela Assessoria de Informática.
8. Para garantir a infra-estrutura do ambiente de TI (Tecnologia da Informação) da Instituição, é indispensável que a instalação de recursos obedeça ao controle de segurança física quanto à localização, ao cabeamento, ao controle de temperatura, à rede elétrica, ao combate a incêndio, ao cumprimento dos patrões de segurança do trabalho, às normas técnicas vigentes e recomendações dos provedores dos recursos.
9. A Assessoria de Informática é responsável pelo inventário e controle dos recursos de tecnologia da informação na Instituição.

> *ANOTE:*
> *Antes de alimentar a impressora com uma nova pilha de papéis, movimente as páginas entre os dedos a fim de retirar a umidade. Isso fará com que as folhas se soltem umas das outras, evitando a alimentação em bloco, que danifica a cabeça de impressão.*

10. Os recursos de informação de prestadores de serviços que são utilizados na Instituição devem possuir uma identificação de patrimônio diferente dos recursos próprios.
11. O manuseio dos recursos de informação (equipamentos) da Instituição deve ser feito preservando sua integridade e funcionamento.

IMPORTANTE:

12. Não é permitida a conexão simultânea de cabo de rede e cabo telefônico para fax-modem. Toda conexão de fax-modem deve ser previamente avaliada pela Assessoria de Informática;
13. As estações de trabalho devem ser protegidas com lacre de segurança, podendo ser abertas apenas por pessoas autorizadas a realizar procedimentos de manutenção ou atualização;
14. Qualquer movimento de estação de trabalho deverá ser avaliada pela Assessoria de Informática e realizada por pessoal autorizado;
15. Todo ponto de rede não utilizado deve estar bloqueado;
16. As salas de reuniões devem ser protegidas com chave, uma vez que a segurança lógica dos pontos de redes localizados nas mesmas, não é ativada;

> *CURIOSIDADE:*
> *Por que minha impressora consome tanta tinta?*
> *Para evitar o desperdício de tinta, configure o controlador de impressão para o tipo de trabalho a ser utilizado. Por exemplo: para imprimir apenas a prova de um documento, utilize o modo rascunho e dê preferência ao modo*

monocromático. Para impressão diária, selecione o modo normal e opte pelo papel comum.

17. A entrada e saída de equipamentos de informática na Instituição devem seguir a norma patrimonial em vigor;
18. Os equipamentos portáteis de propriedade da Instituição deverão ser identificados de forma legível e não removível. Deverão, também, ser acondicionados e transportados de maneira apropriada;
19. As permissões de acessos à rede corporativa e às estações de trabalho, bem como às utilizações de software para aplicações específicas, serão concedidas de acordo com a atividade do usuário. No caso de transferência do mesmo, para outra área, as condições de acesso deverão ser reavaliadas;
20. É expressamente proibido se alimentar próximo aos equipamentos de Tecnologia da Informação.
21. A utilização de programas, aplicativos e softwares em geral devem ser restritos apenas aos autorizados, homologados e de acordo com a lei. É terminantemente proibido o uso de software pirata;
22. O coordenador da área usuária e a Assessoria de Informática são responsáveis pela identificação dos recursos mínimos que o usuário deverá ter acesso para o desempenho de suas atribuições;
23. A cópia de software adquiridos ou desenvolvidos pela Instituição, para uso em computadores não pertencentes às mesmas, deverá ser previamente autorizada pela Diretoria Executiva;
24. A Assessoria de Informática é o responsável pela instalação de novos aplicativos/sistemas e pela alteração da configuração das estações de trabalho;
25. O usuário é o responsável pelo uso de software não autorizado ou não homologado;
26. Quanto à padronização é proibido alterar a configuração funcional (hardware e software) das estações de trabalho.

CONTROLE DE VÍRUS

- *Mantenha o Antivírus ativo e atualizado;*
- *Vacine sempre:*
  Disquetes inseridos no computador;
  Arquivos baixados da Internet;
  Anexos de e-mail;
  Não abra arquivos que possuem DUAS extensões: foto.jpg.pif. É sinal de vírus.
- *Jamais reenvie alerta de vírus para outras pessoas, esta é a forma mais comum do vírus se propagar na rede;*
- *Dica de um antivírus gratuito para usar nos micros de casa é o AVG.*

- O que é um vírus?

  É um programa capaz de se inserir em outros arquivos ou programas e usá-los para reproduzir-se, executar alguma tarefa e, logo depois, transmitir-se. O objetivo de um vírus é, com algumas exceções, causar perdas e danos.

- Que tipo de danos um vírus pode causar à minha máquina?

  Danos Lógicos: Chama-se dano lógico a qualquer dano causado ao conteúdo dos arquivos, bem como ao sistema de armazenamento. Os danos lógicos acarretam perda de informação e, se forem muito sérios, torna necessária a reformatação do disco ou mesmo a reinstalação de todo o sistema.

  Danos Físicos: O desenvolvimento de discos rígidos mais modernos e resistentes tornou os vírus incapazes de danificar o hardware das máquinas infectadas; em alguns casos, pode acontecer perda de dados, reformatação do disco e reinstalação do sistema, o que, apesar de grave, não causaria prejuízo direto ao equipamento. Porém, com o advento das BIOS regraváveis nos computadores mais modernos, alguns vírus, como o *Chernobyl*, são capazes de danificar os dados armazenados nela, deixando o usuário sem outra escolha a não ser a troca ou reprogramação do chip defeituoso.

- Como posso me defender?

  1. As estações de trabalho devem possuir software antivírus padrão instalado, configurado e ativado pela Assessoria de Informática.
  2. Toda estação deve utilizar somente antivírus homologado pela Assessoria de Informática, cabendo ao usuário verificar se ele está ativo e atualizado.
  3. O usuário deve informar imediatamente à Assessoria de Informática qualquer suspeita de contaminação por vírus de computador.
  4. Os usuários jamais devem encaminhar alerta de vírus recebidos por e-mail para grupos de pessoas, uma vez que muitos alertas são os próprios vírus. Estas mensagens devem ser encaminhadas para a

Assessoria de Informática que investigará a veracidade da nota e comunicará a toda a empresa.

5. Todo arquivo anexo dos tipos considerados potencialmente perigoso, que são freqüentemente enviados via correio eletrônico, tais como: arquivos Word (.doc e .dot), arquivos Excel (.xls e .xlt), arquivos PowerPoint (.ppt), arquivos Html (.html e .htm), bem como os de extensões PIF, VBS, EXE, COM, SHS, SCR, CHM e BAT não devem ser abertos com duplo clique, devendo-se antes desanexar e passar o antivírus.
6. O Departamento de Informática deve disponibilizar a versão mais recente do antivírus para instalação nas estações e nos servidores de rede.
7. Cuidados básicos para evitar contaminação de vírus no seu computador:
   - Não abrir e-mail quando não identificado/reconhecido o remetente, pois, quem enviou, pode ser um vírus ou SPAM;
   - Não instalar nada que não tenha certeza da origem, a exemplo de brindes. Nove em cada dez são vírus de acesso remoto.
8. Na observância de dados suspeitos em um arquivo ou comportamento estranho da estação de trabalho, o usuário deverá passar um antivírus.

ACESSO DE PRESTADORES DE SERVIÇOS AOS RECURSOS COMPUTACIONAIS

- Todo prestador de serviço deverá preencher o Cadastro de Terceiros, para ter acesso à rede e sistemas da Instituição;
- O prestador de serviço deverá ter acesso apenas aos dados relacionados com a atividade contratada;
- Equipamentos de terceiros, deverão ser configurados no padrão de estações, definido para a Instituição, antes de ser conectado na rede interna;
- A data limite para criação de contas e senhas, não pode ultrapassar a data do término do contrato.

- Prestadores de Serviço

São todas as pessoas que não pertencem ao quadro funcional da Instituição. São considerados prestadores de serviços: terceiros, empreiteiros, consultores, auditores, estagiários, e empregados de empresas do grupo que não pertencem a Instituição.

1. Os não pertencentes ao quadro efetivo da empresa (consultores internos e prestadores de serviços) devem ser orientados e supervisionados pelo contratante direto, quanto aos aspectos da segurança das informações. O coordenador do contrato será também o responsável pela manutenção dos aspectos de segurança das informações manuseadas pelos mesmos.
2. O coordenador do contrato será responsável por dar ciência aos prestadores de serviços contratados sobre a Política de Segurança da Instituição e, em alguns casos, obter junto ao contratado a assinatura de um termo de sigilo e responsabilidade, principalmente quando a natureza do serviço prestado por este envolver diretamente recursos de informática e/ou informações vitais e críticas da Instituição.
3. O coordenador deve informar à Assessoria de Informática, ou órgãos gestores dos sistemas e bancos de dados, a necessidade de inclusão e exclusão do acesso do prestador de serviço.
4. O coordenador deve zelar pelo uso correto das informações sob a guarda dos prestadores de serviços de sua área.
5. Os prestadores de serviços devem ter identificação diferenciada dos empregados, gerada pelo Sistema de Cadastro de Terceiros, com prazo de validade determinado pelo coordenador ou de acordo com o contrato estabelecido.
6. Os perfis de acesso à rede corporativa devem ser indicados pelo coordenador do contrato e homologados pelo órgão proprietário da informação ou custodiante.
7. O acesso externo para utilização dos recursos da rede deverá ser avaliado pela Assessoria de Informática. No caso de consultores e prestadores de serviços, será necessária a autorização prévia do Departamento ao qual o mesmo esteja prestando serviço.

8. Não é permitido o uso de equipamentos de prestadores de serviços nas instalações da Instituição com acesso à rede corporativa das mesmas. Em caso de força maior, a Assessoria de Informática deve ser acionado para formatação da máquina e configuração com os *softwares* autorizados e homologados.

Como um Prestador de Serviço consegue o acesso à rede da Instituição?

Através do preenchimento do formulário de Cadastro de Terceiros e de um *login* de acesso individualizado.

- Cadastro de Terceiros

9. Antes de ser criado um *login* de acesso para o prestador de serviços, o mesmo deverá preencher o formulário Cadastro de Terceiros, disponível na rede.
10. Cabe ao coordenador ou supervisor da prestadora de serviço acessar o Cadastro de Terceiros e indicar o desligamento do prestador de serviço, a fim de ser bloqueado o acesso à rede da Instituição.

ACESSO REMOTO & COMPUTADOR MÓVEL

- O computador móvel requer cuidados especiais, uma vez que possui o valor físico do equipamento, e o valor das informações;
- Existem situações especialmente perigosas para o transporte de notebooks, como por exemplo, trânsito em saguões de aeroportos, salas de espera, convenções, palestras, hotéis e demais locais onde haja uma freqüente concentração de executivos;
- Ao perceber que ocorreu o roubo, o usuário deve registrar a queixa policial e comunicar à Assessoria de Informática, para bloquear imediatamente o acesso de rede entre o equipamento e a empresa.

São considerados computadores portáteis:

Notebook, palmtop, POS (*point of Sale*), etc...

1. Quando do recebimento do computador portátil, os executivos e empregados deverão assinar o Termo de Custódia, contendo os direitos e deveres quanto à utilização, posse e guarda desses equipamentos.
2. Estes equipamentos devem ser utilizados única e exclusivamente para execução das atividades relacionadas à empresa.
3. O acesso remoto limita-se exclusivamente para realizações de atividades críticas, que envolvam manutenção de sistemas ou acesso à informação fora das dependências da Instituição.
4. Quando em trânsito, o usuário não deve emprestar, perder de vista ou deixar o equipamento em mãos de pessoas não relacionadas ao quadro de funcionários da Instituição.
5. O usuário é o responsável pelo uso de *software* não autorizado ou não homologado, instalado no equipamento.
6. Todas as informações armazenadas no equipamento serão de propriedade da Instituição, não devendo, em hipótese alguma, ser distribuídas, copiadas, compartilhadas ou vendidas para quem quer que seja, em qualquer meio, seja impresso, magnético ou transcrito.
7. Em caso de auditoria, a Instituição reservar-se-á o direito de supervisionar todos os dados transmitidos/recebidos a partir destes equipamentos, não caracterizando quebra de sigilo, uma vez que os recursos colocados à disposição são de propriedade da mesma.
8. Em caso de falha em qualquer dispositivo do equipamento em questão, o usuário não deverá procurar assistência técnica ou fazer qualquer substituição de componentes (baterias, carregadores, antenas, etc.) sem a autorização prévia da Assessoria de Informática.
9. A utilização de equipamentos portáteis/transportáveis tem o objetivo de facilitar o trabalho de usuários que passam grande parte do tempo em locais fora da Instituição (Diretores, Coordenadores, administradores de sistemas, áreas técnicas específicas e situações especiais de sobreaviso).

- E se eu for roubado?

10. Em caso de roubo, furto, perda total ou parcial do equipamento recebido, o usuário deverá comunicar imediatamente a sua gerência e à Assessoria de Informática. Caso o sinistro tenha ocorrido fora das dependências da empresa, deverá ser providenciado o registro de ocorrência junto à autoridade policial legal.
11. O acesso às redes corporativas somente será permitido a equipamentos homologados e cadastrados pela Assessoria de Informática.
12. A liberação do uso de aplicações remotas e de transmissão de dados só será realizada após aprovação do coordenador do departamento solicitante e homologação da Assessoria de Informática.
13. Senhas usadas para acessar os sistemas da Instituição não devem ser divulgados ou expostos a pessoas não autorizadas, ficando o usuário responsável pelo sigilo destas informações.
14. Se o equipamento portátil for compartilhado por vários usuários, o coordenador deverá emitir um termo de custódia e anexar a relação de todos os usuários autorizados. Os *logons* de acessos autorizados serão revalidados anualmente pela Assessoria de Informática.

SALA DE BACKUP

- O acesso ao CPD deve ser exclusivamente para pessoas cadastradas;
- As portas de acesso ao CPD devem estar permanentemente trancadas e o uso de câmaras são recomendadas;
- Não devem ser armazenados materiais inflamáveis na sala do CPD;
- As fitas de backup devem ser protegidas contra destruição e/ou furto;
- Testes para restauração de dados devem ser, periodicamente, testados.

1. Por medida de segurança, é expressamente proibida a entrada de funcionários e terceiros, que não tenham autorização expressa, na sala do CPD da Instituição. Os funcionários autorizados a acessar as referidas salas devem ser cadastrados no Sistema de Controle de Acesso.
2. Caso seja necessária a entrada de alguma pessoa não cadastrada no Sistema, a mesma deverá ser autorizada pela Assessoria de Informática. Ao entrar na sala, deverá assinar o "Livro de Controle de Acesso", que fica localizado no seu interior. Neste livro, deverão constar, no mínimo, os seguintes campos:
   - Nome;
   - Registro funcional (para funcionários) ou RG (para não funcionários);
   - Empresa;
   - Data;
   - Hora da entrada;
   - Hora da saída;
   - Motivo;
   - Assinatura do visitante;
   - Assinatura do funcionário acompanhante.
3. É expressamente proibida a permanência de pessoas não cadastradas na sala do CPD fora do horário de expediente. Caso haja a necessidade desta permanência, a visita deverá ser previamente agendada.
4. É terminantemente proibida a estocagem, mesmo que por um período curto de tempo, de qualquer material ou equipamento que não esteja relacionado com a operação das salas em questão.
5. É proibida a entrada de alimentos, bebidas, líquidos inflamáveis ou não e materiais que produzam pulsos eletromagnéticos (ímãs e similares) na sala do CPD.
6. Caso haja a necessidade da retirada de qualquer informação dos servidores, só poderá ser realizada após a autorização formal do proprietário/gestor da informação.
7. Obras:
   a) Qualquer obra deverá ser previamente acordada para que os riscos com a operação do CPD sejam avaliados e, só depois, seja decidida a paralisação ou não do mesmo;
   b) Em casos de execução de obras, os equipamentos deverão estar totalmente protegidos dos riscos provenientes da mesma;

c) A obra deverá ter um acompanhamento de um responsável pela área de TI e um outro pela área de manutenção.

8. No caso de desaparecimento ou dano causado a algum equipamento, por negligência ou não cumprimento da norma, por parte de algum empregado, estagiário ou prestador de serviço, este será responsabilizado e estará sujeito a sanções administrativas.
9. A Planilha de Inventário deverá ser imediatamente atualizada pelo pessoal autorizado, quando da colocação ou retirada de qualquer material da sala de guarda de materiais, equipamentos e backup.

SEGURANÇA FÍSICA & LÓGICA DOS SERVIDORES

- Os servidores possuem dados críticos e relevantes da organização, por isso devem ficar em locais seguros.
- É necessário garantir a integridade física e lógica dos servidores, a fim de evitar prejuízos financeiros.
- Todos os servidores devem possuir antivírus instalado e atualizado diariamente.
- Apenas as pessoas autorizadas, deverão possuir senhas de acessos aos servidores, com perfil de administração.

1. O usuário deve manter sigilo sobre as informações estratégicas, vitais e confidenciais da Instituição.
2. As informações classificadas como críticas, que serão disponibilizadas para realização de trabalho fora das dependências da Instituição (sejam elas via e-mail, disquetes ou outro meio eletrônico), deverão conter senhas para que seja garantida a integridade, a disponibilidade e a confidencialidade. Nesse caso, é indicada a utilização de programas de criptografia.
3. O usuário deve informar ao seu coordenador quando informações ou aplicações críticas forem encontradas sem tratamento de segurança correto. Este deve informar a ocorrência à Assessoria de Informática.
4. Os equipamentos "servidores" terão identificação própria de inventário em local visível e não removível, onde, com base nesta identificação, será efetuado o controle de entrada e saída ou transferência do respectivo ativo.

MOVIMENTAÇÃO

5. A movimentação de servidores é restrita à Assessoria de Informática.
6. É proibido se alimentar e fumar próximo aos servidores ou áreas consideradas críticas, a fim de evitar incidentes que venham causar danos indesejáveis.
7. Todos os servidores, roteadores e demais equipamentos da rede devem possuir data e hora oficiais atualizadas e sincronizadas.
8. A lista de softwares autorizados para uso na Instituição deve estar sempre atualizada e disponível para consulta dos usuários, pela Assessoria de Informática.
9. As aplicações críticas devem estar armazenadas na rede, sempre em diretórios protegidos, a exemplo do disco L.
10. As configurações dos softwares em operação na Instituição devem sempre incorporar as correções implementadas pelos fabricantes e homologadas pela Assessoria de Informática.
11. As informações sobre as estruturas lógicas e físicas da rede devem ser armazenadas em documentos separados, mantidos sempre atualizados, descrevendo, no mínimo, a topologia e os endereços dos componentes.
12. As informações relevantes e relacionadas às atividades de trabalho na Instituição devem ser armazenadas no servidor da rede e não nos discos das estações.

13. Devem ser removidos dos servidores da rede, os arquivos que não sejam mais necessários ou que não se refiram a assuntos de trabalho, a fim de ser liberado espaço em disco.
14. O acesso para administração de sistemas e banco de dados em servidores deve ser permitido somente para pessoas autorizadas e através de estações homologadas, com autorização de acesso configurada pela Assessoria de Informática.
15. A integridade física de servidores de rede e de equipamentos de comunicação (modem, roteador, switch, etc.) é fator primordial para a continuidade dos serviços. Para sua segurança, tais recursos deverão ser instalados em ambiente especial, reservado e exclusivo, com acesso restrito e controlado.
16. O pessoal de apoio de serviços gerais deve ter acesso aos ambientes de processamento e comunicação (modem, roteador, switch, etc.) somente com autorização e em horário previamente determinado. Além disso, deverá ser acompanhado por um responsável durante sua permanência no referido local.
17. As áreas de equipamentos críticos da rede corporativa da Instituição devem ser de acesso restrito às pessoas autorizadas ou acompanhadas por estas.
18. Apenas os administradores de rede, operadores e técnicos autorizados deverão possuir senhas para acesso aos servidores.
19. Todos os servidores devem possuir sistema operacional, sistema de backup e antivírus homologados pela Assessoria de Informática.

BACKUP & PLANO DE CONTIGÊNCIA

- O BACKUP garante a recuperação dos dados em caso de incidente.
- Existem várias formas de se fazer um backup, e o mais importante é manter atualizado com a última versão.
- Jamais devemos acreditar que a tecnologia é infalível, por isso é sempre necessário um plano de contingência.
- Sistemas considerados críticos, devem possuir um plano de contingência, a fim de evitar a indisponibilidade do mesmo.

BACKUP

São cópias de segurança, geralmente mantidas em disquetes, fitas magnéticas ou CD-ROM, que permitem o resgate de informações importantes ou programas, em caso de falha do disco rígido.

1. As informações importantes relacionadas às atividades de trabalho na Instituição devem ser armazenadas no servidor da rede, de forma que seja realizado backup das mesmas.
2. Os usuários poderão solicitar à Assessoria de Informática, através do Suporte ao Usuário, a restauração dos dados mediante a autorização do proprietário dos referidos.
3. O backup das informações existentes nas estações de trabalho é de total responsabilidade do usuário, que deverá usar disquetes ou CD-ROM.
4. O gestor da informação deve estabelecer um acordo com a Assessoria de Informática, durante a fase de desenvolvimento, para recuperação de backup em caso de falha. Este acordo deve contemplar caracterização de criticidade de informação e tempo máximo para a disponibilização da mesma, assim como a peridiocidade, o tempo de retenção das mídias e o tipo de backup.
5. É responsabilidade da Assessoria de Informática operacionalizar o backup, garantindo a integridade do mesmo por meio de testes periódicos e disponibilizar para usuários a lista atualizada dos seus servidores, discos e pastas que são contempladas pelo backup.
6. As mídias de backup devem ser armazenadas em cofres especiais, que garantam a proteção das mesmas em caso de incêndio, enchente ou vazamento de gás. Na impossibilidade do uso de tais cofres, deve ser gerada mais uma cópia de segurança para ser armazenada em local diferente, a salvo de possível contingência.

DICA:
Disco sem sistema *- Se, ao ligar a máquina, surgir a mensagem "Disco sem sistema ou defeituoso", veja se não foi esquecido um disquete no drive A. Nesse caso, o micro tentou carregar o sistema operacional a partir do disquete e, não o encontrando, cancelou a inicialização. Se for esse o problema, retire o disquete e pressione alguma tecla ou religue a máquina para que ela funcione. Se a mensagem aparecer sem que haja um disquete no drive A, um problema grave pode ter ocorrido no disco rígido.*

PLANO DE CONTIGÊNCIA

7. Os planos de contingência devem ser testados e reavaliados periodicamente.
8. A Assessoria de Informática deve manter atualizados os procedimentos dos planos de contingência.
9. Todos os recursos a serem disponibilizados em produção devem ser inventariados e previamente homologados em ambiente de teste.
10. A disponibilidade de recursos críticos deve estar assegurada pela existência de um plano de contingência.
11. Os equipamentos devem ser submetidos a uma rotina de manutenção preventiva. Os equipamentos e aplicações envolvidos em processos críticos de produção têm prioridade no atendimento.
12. Os procedimentos de testes devem ser realizados em massa de dados específica.
13. A disponibilidade ininterrupta de recursos críticos deve estar assegurada pela existência de backup e de um plano de contingência.